UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
MANHATTAN DIVISION

JAMES CAPLAN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

YAHOO INC.,

Defendant.

Case No. 1:25-cv-02943

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff James Caplan, individually and on behalf of all others similarly situated individuals, asserts the following against Defendant Yahoo Inc. ("Yahoo") based upon personal knowledge, information and belief (where applicable), and the investigation of counsel.

SUMMARY OF ALLEGATIONS

1. Yahoo is considered one of the earliest internet companies, rising to prominence through its email service and search engine capabilities. With that prominence, Yahoo is also well known for their back-to-back data breaches from over a decade ago, which compromised the account information of nearly every Yahoo email user.

2. Today, Yahoo provides much more than email domains and search functions. Starting in the 2000's, Yahoo began acquiring marketing and ad tech companies to develop a user-based online targeting business. This began with its acquisition of Right Media in 2007 and continued through the buyouts of Flurry Analytics and BrightRoll in 2014.

3. These acquisitions were so lucrative it ultimately led to the acquisition of Yahoo by Verizon in 2017 for $4.83 billion. Verizon's CEO at the time, Lowell McAdam, said the acquisition of Yahoo "put Verizon in a highly competitive position as a top global mobile media company and

help[ed] accelerate [its] revenue stream in digital advertising."

4. Yahoo's value was derived from the new forms of persistent, user-based online tracking it developed through these acquisitions. Specifically, in 2020—after Apple and Google announced they would eventually phase out third-party cookies and Apple would restrict the use of mobile identifiers—Yahoo released a new, unified way to track users across platforms and devices.

5. This solution is called Yahoo ConnectID (formerly known as "Verizon Media Connect ID"), built on Yahoo's Identity Graph. Rather than relying on cookies or mobile identifiers, the Yahoo ConnectID is an email-based persistent identifier. When a user logs in or provides an email (a form of personally identifiable information ("PII")) to an online service offered by Yahoo or one of its partners, Yahoo intercepts and assigns a Yahoo ConnectID to that user based on their email address.

6. Yahoo promotes this as a "privacy-centric" and "[p]rivacy first" identity solution. It is anything but. The Yahoo ConnectID is privacy-invasive because it is a work-around to privacy mechanisms designed to prevent this type of user-based tracking. For instance, Safari and Firefox browsers both restrict the use of third-party cookies, but the Yahoo ConnectID defeats these privacy precautions by assigning a persistent identifier directly mapped to the users email address and accompanying PII without the use of traditional third-party cookies, instead relying on first-party cookies implemented onto websites. Similarly, if a user cleared their cookies or other tracking technology on their browser, this too would not stop Yahoo because it will simply identify them again the next time they log-in to a website that recognizes ConnectID with their email address.

7. Yahoo does not tell its users of the ConnectID, how it works, or that this identifier is tied directly to their email addresses and assorted PII.Yahoo's Privacy Policy makes no

mention—at all—of Yahoo ConnectID. In fact, their policy expressly states that it does "not share personally identifiable information (like phone number or email address) with . . . partners, such as publishers, advertisers, ad agencies, or analytics partners." This is deceptive. It's true, Yahoo does not disclose email addresses directly. Instead, Yahoo intercepts and maps the user's email address directly to a ConnectID, a persistent identifier that it does share with others to track users across the internet and various websites. This translation is akin to (and no better than) sharing the email address itself.

8. Yahoo's role as a centralized identity broker allows it to uniquely identify individuals and recognize them across websites and devices—exactly what privacy-preserving mechanisms are meant to prevent, and all without user consent. Yahoo has confirmed that, through Yahoo ConnectID, it has successfully identified over ***300 million*** logged-in users.

9. Worse, Yahoo does not simply track the identify of its users, but it creates ***profiles*** for the users, a key feature used to fuel its lucrative advertising business. As described herein, Yahoo combines the Yahoo ConnectID with private data it obtains through its apps, websites, and other services—as well as similar private data from its customers/partners—to create comprehensive user profiles. This data comes from: (1) Yahoo owned web properties and those of its subsidiaries, like Flurry, who had a stronghold on data from "70% of the apps on the average smartphone"; (2) Yahoo's own advertising and analytics solutions, which are incorporated and used by developers and advertisers; (3) Yahoo's machine-learning and AI solutions, which enrich and analyze data to derive even more information about the user; and (4) Yahoo's role as a demand-side platform ("DSP") and supply-side platform ("SSP") in the world of real-time bidding ("RTB"). Yahoo uses this massive pool of profile data to further improve its ability to identify and target unique users with advertisements by updating and improving the models and algorithms that

do so.

10. Through Yahoo ConnectID—and complimentary products (described briefly above)—Yahoo has been secretly harvesting and monetizing directly identifiable user data from millions of U.S. residents without their knowledge and consent.

11. Yahoo's interception of the contents of their communications with third parties through its tracking technology and installation of a tracking device on each of the websites they use across the internet violates New York's General Business Law, Pennsylvania's Wiretapping and Electronic Surveillance Control Act, as well as other laws.

PARTIES

A. Plaintiff

12. Plaintiff James Caplan is a resident of Pennsylvania

13. Plaintiff Caplan has several online accounts at sites that use Yahoo's tracking technology, which he created using his email, including an account with CBS Sports.

14. When Plaintiff Caplan visited these websites and logged in with his email address, Yahoo intercepted his email and assigned or attributed his information to an existing Yahoo ConnectID.

15. Yahoo used this Yahoo ConnectID—alongside its other ad and analytics technology—to track Plaintiff Caplan across the internet and develop a unique user profile. Through this technology, Yahoo intercepted at least (1) Plaintiff's searches; and (2) full-string URLs revealing what Plaintiff Caplan was viewing and interacting with on web properties. Yahoo processed this data and stored it on its own servers—alongside his Yahoo ConnectID—for its own benefit and monetary gain. It also used this data for training its machine learning models and algorithms to better target online users.

16. Plaintiff Caplan did not consent to Yahoo intercepting his unique identifiers and other personal data, assigning, and using unique identifiers to track him across internet-enabled services and devices, or intercepting and using the contents of his private communications for profit.

B. Defendant

17. Yahoo is a Delaware corporation with its principal place of business located in New York, New York.

18. Yahoo knowingly and intentionally developed persistent, unique identifiers to track Plaintiff and Class Members across internet-connected services, despite knowing these types of identifiers were at odds with users' expectation of privacy.

19. Yahoo knew that its identifiers, especially Yahoo ConnectID, circumvented existing privacy protections (like the deprecation of third-party cookies) because it developed this identifier specifically as an alternative to such privacy-preserving mechanisms.

20. Yahoo offered these services to websites, mobile applications, advertisers, data brokers, and other internet-connected services so that it would have a unique way of tracking Plaintiff and Class Members across devices and platforms.

21. Yahoo knowingly and intentionally used its identifiers, and data associated with it, to profile online users and facilitate targeted advertisements for profit.

<u>JURISDICTION AND VENUE</u>

22. Jurisdiction is proper under 28 U.S.C § 1332(d) because: (1) the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, (2) there are more than 100 putative members of the Class, and (3) a significant portion of Class Members are citizens of a state different from Yahoo.

23. This Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(a) because the amount in controversy in this case exceeds $75,000 and this action is between citizens of different states. Plaintiff is a resident of Vermont whereas Defendant is a Delaware entity with its principal place of business in New York.

24. This Court has personal jurisdiction over Yahoo because Yahoo's principal place of business is in New York.

25. Venue is proper under 28 U.S.C. §1391(b), (c), and (d) because Yahoo is headquartered in this District and subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

I. BACKGROUND OF USER TRACKING

26. Over a decade ago, Apple announced it would no longer allow app developers to intercept "UDIDs" which are unique identifiers. These persistent identifiers were deprecated because they are seen as privacy intrusive—they cannot be reset and were used to facilitate targeted advertising.

27. This trend continued. Starting in 2020, Apple and Google announced the eventual deprecation of advertising identifiers (IDFA and ADID) and third-party cookies in favor of more privacy-preserving mechanisms.

28. The loss of some of the most common unique identifiers raised serious concerns within the multi-billion-dollar digital advertising industry. Digital advertisers relied on these identifiers and cookies to uniquely identify individuals who use their products and services—and other entities' products and services—to serve targeted advertisements to individuals, based on profiles of information reflecting web and app activities indexed to unique identifiers present in third-party cookies.

29. For instance, a mobile app developer would use identifiers like the IDFA and ADID created by iOS and Android phones to track user activity across their mobile application, understand what actions users took and their preferences, interests, and other information. The company would then send that information to an advertising company, such as Google, to serve targeted advertisements to that customer using this unique identifier.

30. Proposed solutions to make up for these unique identifiers and third-party cookies were not nearly as effective. For instance, some companies sought to track user "sessions" (i.e., one interaction with the webpage until the user closes out) in lieu of other unique identifiers. However, this alternative was not nearly as powerful as directly tracking an individual at the user or device level.

II. YAHOO'S UNIQUE AND PERSISTENT CONNECTID

31. Yahoo itself was well aware of the eventual deprecation of third-party cookies, which is precisely why it created Yahoo ConnectID.

32. Yahoo advertised its persistent identifier as a "future-proofed" solution because Yahoo designed it as a work-around that can overcome cookie-blocking and deprecation such as those implemented as part of Apple's iOS updates in May of 2021.

33. Yahoo created Yahoo ConnectID in December 2020 ahead of Apple's implementation of this change.

34. Every individual who uses a Yahoo owned property (e.g., Yahoo Mail, Yahoo Sports, TechCrunch, AOL, Engadget, etc.) is assigned a unique ConnectID, which is tied directly to the users' email addresses (a form of PII) and allows them to be consistently tracked across the internet.

35. But Yahoo users aren't the only individuals who have a ConnectID. Yahoo also

assigns a ConnectID to ***non-Yahoo users***. When Plaintiff and Class Members visit a website or internet-connected service that enables ConnectID (regardless of whether they are a Yahoo user), Yahoo intercepts their email addresses, which is typically hashed using SHA-256.

36. Next, Yahoo processes and analyzes whether the user has an existing ConnectID using this hash value.

37. If the user does not have an existing ConnectID, then Yahoo creates a new one. Yahoo then stores the ConnectID—typically in the user's local storage—and returns it to the website or internet-connected service.

38. The ConnectID, therefore, permits consistent user-level tracking—based off directly identifiable email addresses—across the internet as person moves across different websites and shares additional sensitive information in the process.

39. Importantly, ConnectIDs are ***not*** a form of anonymized data.

40. Rather, this data remains identifiable because it is directly tied to actual PII.

41. Thus, while ConnectID does not itself contain the user's actual email address or phone number, it serves as the functional equivalent of those values based on its direct mapping to them.

42. Yahoo's use of hashing in this process does not protect users' emails addresses or render the data anonymous. Indeed, this methodology has been ***repeatedly criticized***, including by the Federal Trade Commission ("FTC").

43. The FTC has confirmed that "hashing" email addresses that always return the same identifying number (like here) is both an "old" and "flawed" methodology because the hashes are not "anonymous" and "can still be used to identify users, and their misuse can lead to harm." It cautions: "[c]ompanies should not act or claim as if hashing personal information renders it

anonymized." Here, based on how ConnectID is configured, every time a user enters the same email address or a website or platform, the same hash value and thus ConnectID is used—exactly what the FTC cautions against.

44. Especially problematic, ConnectID is a ***stronger*** identifier than those that previously existed. For instance, first-party cookies are typically limited in that they only track a user on one specific website. ConnectID goes ***further*** by tracking users across ***all*** websites and ***all*** apps using this identifier.

45. Similarly, if a user cleared their browsing history, cookies, and other identifiers, this would reset most traditional cookies. ConnectID, however, bypasses this functionality as it would simply reassign the same ConnectID whenever the user logged-in again. This makes it possible to create highly profitable identity profiles, by aggregating data across all apps and websites a person uses, at the expense of the individual's right to privacy.

46. ConnectID is also linked to the "puid" cookie, a first-party cookie that acts as a domain-specific user identifier stored in local and/or cookie storage on the user's device.

47. Yahoo's ConnectID has become "one of the world's most popular cookieless identifiers" and is implemented "across nearly 50,000 publisher domains[.]" It is used across websites, apps, and even connected TVs. For instance, Paramount, Tubi, and NBCUniversal all have partnerships to use Yahoo ConnectID, as well as its Next-Gen Solutions (discussed further below).

48. Yahoo's Connect ID can also be used in connection with other third-party data platforms—like Live Ramp, Epsilon, Adobe, Acxiom—meaning these other third parties are also tracking users via ConnectID. ConnectID has been used to successfully identify over 300 million unique, logged-in users.

III. HOW CONNECTID IS INTEGRATED ON WEB PROPERTIES

49. Anyone can incorporate ConnectID, including website and app developers, publishers, and advertisers. All that is required is registering with Yahoo and following one of Yahoo's integration instructions.

50. Yahoo publicly describes five methods to integrate its Connect ID: (1) Prebid method; (2) JavaScript method; (3) server-to-server method; (4) Google Secure Signals; (5) LiveRamp ATS; and (5) Amazon CxM.

51. Alarmingly, Yahoo openly tells publishers that they need not concern themselves with obtaining user consent because it already provides "multiple mechanisms" for users to manage their privacy choices. This is misleading at best. Yahoo's Privacy Policy makes no mention of sharing directly identifiable email addresses and, in fact, represents that email addresses will not be shared. Plaintiff and Class Members had no way of knowing they were being uniquely identified and tracked across the internet through their email addresses.

A. The Prebid Method

52. Yahoo's Prebid method is designed for publishers. Publishers register with Yahoo and configure the ConnectID module within their existing Prebid.js implementation.

53. This module enables Yahoo to associate users with a Yahoo ConnectID and pass that identity into the bidstream during RTB, thus facilitating cross-site targeting even in environments where third-party cookies are unavailable.

54. Specifically, this framework enables Yahoo to intercept SHA-256 hashed email address, which is used to generate a new Yahoo ConnectID or match to an existing one.

55. When an ad call is made to SSPs, including Yahoo's SSP, the Yahoo ConnectID is included in the OpenRTB request payload. This can be observed in network traffic, where the

ConnectID is listed under the “user.ext.eids” array with “source”: “yahoo.com”. As described in Section IV, the OpenRTB request payload reveals additional information about the user beyond their identity.

B. The Javascript Method

56. The Javascript method is just a more direct integration, as it is incorporated in the source code level of developers’ or advertisers’ websites. Entities register with Yahoo, but instead of enabling ConnectID through the Prebid.js implementation, they use node package manager (“npm”) to install the module in the terminal and embed the Javascript code provided by Yahoo directly into their source code.

57. Once enabled on the web property, Yahoo intercepts SHA-256 hashed or “raw email” addresses. Yahoo processes this information and assigns or returns the ConnectID, which is typically stored in the user’s local storage, and returns it back to the entity.

C. Server-to-Server Method

58. The server-to-server method works similarly to the Prebid and Javascript methods but uses tokens and initially transmits this data between two back-end servers, hence the name.

59. First, the entity obtains OAuth credentials through Yahoo to authenticate API requests. Once the credentials are set up, the entity generates a JSON Web Token (JWT), which is submitted to a Yahoo endpoint to obtain an “access token” so the entity can send future API requests.

60. Next, through Yahoo’s integration, it intercepts through an API call the SHA-256 hashed email address, as well as other parameters, such as a client_id. Yahoo then assigns or identifies the ConnectID, which it returns to the entity.

D. Google Signals Method

61. Entities with a Google Ad Manager account can integrate Yahoo's ConnectID through the Secure Signals feature. This involves signing into their account, navigating to Inventory > Secure Signals**,** enabling Yahoo ConnectID by toggling its status, selecting a method for deploying the signal collection script (either Google auto-deployment or the Prebid UserID module), and saving the settings.

62. Once configured, the ConnectID script is up and ready to go. The script generates first-party cookies when users interact with the entity's website—including "yahooid"—which contains SHA-256 hashed email addresses. The ConnectID script reads the value and uses it to generate, or identify an existing, ConnectID.

E. Amazon CxM Method

63. Like the Google Signals Method, entities can "seamless[ly]" and with "little effort" incorporate ConnectID simply by changing settings in the entity's Amazon Publishers Service.

64. Once configured, the ConnectID script is up and ready to go. The script generates first-party cookies when users interact with the entity's website—including "yahooid"—which contains SHA-256 hashed email addresses. The ConnectID script reads the value and uses it to generate, or identify an existing, ConnectID.

F. LiveRamp ATS Method

65. Similarly, enabling ConnectID through LiveRamp requires "minimal effort" but "unlock[s]" and allows entities to "better monetize their supply" through "additional demand in Yahoo DSP for the cookieless world.

66. Yahoo offers to assist customers in enabling ConnectID with LiveRamp. When completed, LiveRamp—through its Authenticated Traffic Solution—picks up the ConnectID when

email addresses are intercepted on the entity's website. Thus, this is yet another way users are tracked through ConnectID when they visit a participating entity's website.

IV. YAHOO USED CONNECTID AND USER PROFILES TO FUEL ITS BUSINESS

67. Yahoo created the ConnectID precisely because of its synergy with its existing analytics, advertising, and AI products. Through each of these products, Yahoo benefits directly from ConnectID, and therefore from users' PII (i.e., email addresses), and other private online activity. These products are described below.

68. **Yahoo Dot Tag and Pixel API.** Yahoo's Dot Tag and Yahoo's Pixel API are mechanisms embedded on webpages that are used to intercept users' activity on the webpage. This includes interactions like page views, clicks, form submissions, conversions, and other activity tracked through what are known as "events." These mechanisms also collect persistent identifiers, such as cookies and device identifiers. The information intercepted is used to provide robust user identification and develop user profiles, described further below, all of which can be associated with a user's ConnectID.

69. **Yahoo Analytics.** Similar to Yahoo Dot Tag and Yahoo's Pixel API, Yahoo Analytics is used to intercept and track users' activities across the web. The information intercepted includes identifying information, such as cookies, device identifiers, and IP addresses, as well as full-string URLs reflecting users' private online activities, such as their searches and the pages they view across the internet. Advertisers and developers can associate this information with Yahoo's user profiles and thus the user's ConnectID.

70. **Yahoo's User Profiles.** Yahoo's ConnectID is not just an identifier product. Rather, through ConnectID, Yahoo creates a profile of each logged-in user who accessed its own properties, including Yahoo Mail, Yahoo Sports, Yahoo Connected TV, TechCrunch, AOL,

Engadget, etc. Yahoo logs every signal about the user, including for example, their searches, purchases, and location information. Yahoo collects all of this engagement data as a first-party, synthesizes the data, and compiles it into a "comprehensive and deep" profile for each user. Yahoo therefore, is able to maintain a "user match pool" that "preserves the identity and preferences" of its users across all the properties it owns or operates. So far, Yahoo is maintaining user profiles for at least 300 million logged-in users.

71. Further, Yahoo is constantly "enrich[ing]" the ConnectID user profiles by joining its first-party data with data from other sources. Yahoo accomplishes this through its "Interoperability Program" which is Yahoo's efforts to match ConnectID with different identifiers created by other parties. For example, when an ads publisher implements ConnectID and passes user data to Yahoo along with other different identifiers, Yahoo would match ConnectID with these identifiers and then use the data to supplement the user profile linked to the user's ConnectID. Yahoo applies the same process to advertisers as well. According to Yahoo, it is able to match its ConnectID with identifiers from "all leading CDP and DMP providers," including but not limited to those from "Acxiom, Adstra, Equifax IXI, Experian, Neustar, TransUnion, Throtle and Epsilon." If a client uses an identifier that does not match with ConnectID within Yahoo's existing Interoperability Program, Yahoo would then work with the client to "bring those [identifiers] in," "translate those into ConnectID," and "activate through the entire [Yahoo] stack." Still, Yahoo does not stop there—it also allows its clients to provide PII such as phone number or physical address to match directly with ConnectID. Because the ConnectID user profiles ingest data from all of these sources along with various other identifiers, they have "resolution to an individual" rather than just to email accounts.

72. **Yahoo's Supply-Side Platform.** Previously, Yahoo participated in RTB as a supply-side platform (SSP), which is how publishers sell their ad inventory. Yahoo as an SSP—and its SSP partners—recognize and use ConnectID, which they transmit with bid requests received by DSPs. SSP's that recognize ConnectID include Pubmatic, Magnite, and InMobi Advertising.

73. **Yahoo's Demand-Side Platform.** Also, as a part of RTB, Yahoo acts as a demand-side platform (DSP). As a DSP, Yahoo allows advertisers to bid on and purchase ad space. Publishers and SSPs often include ConnectID in the bid request (described above), as well as other identifiers like cookies. Yahoo uses ConnectID to link the ad target (i.e., who will see the ad) to an existing user profile in Yahoo's systems, enabling its advertising customers to target users at an individualized level. Thus, ConnectID directly contributes to how successful Yahoo's DSP customers are in serving targeted ads, which results in profits to Yahoo.

74. **Creating Audiences.** Yahoo's customers can leverage ConnectID in conjunction with Yahoo's suite of advertising products to maximize their ad spending and ability to target individuals at the user-level. Yahoo boasts that these customers have access to over 4 trillion data points and 450+ "accurate audience segments." Customers can use these existing audiences, create custom audiences, or predictive audiences (powered by machine learning, described below)—all linked to ConnectID—to target individuals across Yahoo's ecosystem, including in RTB. Customers can also share their own first-party data to "seamlessly match" it with ConnectID to further target these individuals.

75. **Machine Learning & AI.** Yahoo uses its ConnectID Identity Graph—comprised of millions of "known users"—to train AI and machine learning algorithms that profile and target unknown individuals, a product Yahoo refers to as "Next-Gen." As the ConnectID seeks to identify

logged-in users of Yahoo and its partners' properties, the Next-Gen solution seeks to identify those who did not log in while accessing these properties by inferring the identity and preferences of the individual from existing data through machine learning algorithms. For example, when an unidentified user engages in activity, such as browsing for Chicago Bulls merchandise, Yahoo's Next-Gen models compare this behavior against the patterns of known users to infer traits like interests, demographics, or purchasing intent. In effect, Yahoo leverages its vast surveillance dataset to make behavioral predictions about individuals even when it lacks direct identifying information about them. Yahoo's Chief Revenue Officer, Elizabeth Herbst-Brady, refers to this as a solution for "advertisers and publishers" to be "successful" when confronting "non-addressable inventory" (i.e., users for whom there is no ConnectID). As Yahoo's own Vice President on Ads Data acknowledges, Yahoo relies on the ConnectID user profile data as training data to constantly finetune its Next-Gen models.

REAL-WORLD EXAMPLES

76. Plaintiff Baker, like other Class Members, frequently visits online websites, including CBS Sports. When a user visits CBS sports (at the following domain: https://www.cbssports.com/), users are not prompted to agree to cookies or other forms of online tracking.

77. As soon as a user visits this website, Yahoo begins tracking the user. This can be observed through network traffic, which sends data to "ups.analytics.yahoo.com." Yahoo receives an "A3" cookie as well as the "IDSYNC" cookie. The A3 cookies is a unique identifier used by Yahoo for advertising and personalization. The "IDSYNC" cookie allows Yahoo and other similar data brokers to share (i.e., "sync") their unique identifiers with one another so both companies can successfully identify and target the user. On the CBS Sports website, it is clear that Yahoo is

syncing identifiers with, at least, Rubicon—a known SSP. Yahoo continues to do this as CBS Sports users continue to navigate to other web pages on the website. Upon information and belief, Yahoo uses this information to sync CBS Sports users with their ConnectID.

78. CBS Sports is also an ad publisher and therefore relies on SSPs to sell ad space—most notably, the company GumGum. When users, including Plaintiff Baker, log into CBS Sports their identifiers—such as Yahoo's ConnectID—are transmitted to GumGum during RTB. This can be observed in the payloads sent from CBS Sports to GumGum. GumGum then shares this information with DSPs, like Yahoo, which use it to bid on available ad inventory. Because Yahoo maintains user profiles tied to ConnectID, this enables it to serve targeted advertisements based on users' identities and behaviors. Thus, Yahoo has additional insight about the user, unlike competing DSPs.

79. Walmart's website (available at: https://www.walmart.com/) and HealthLine's website (available at: https://www.healthline.com/), both of which Plaintiff Baker also used, also rely on Yahoo Analytics. Yahoo again intercepts to its domain "sp.analytics.yahoo.com" the A3 cookie and IDSYNC cookie, both of which are used for identification purposes. On Walmart specifically, Yahoo continues to intercept and track user's interactions, including full-string URLs reflecting their searches and pages they view. Upon information and belief, Yahoo uses this information to sync Walmart and HealthLine users with their ConnectIDs.

PLAINTIFF AND CLASS MEMBERS HAVE A REASONABLE EXPECTATION OF PRIVACY

80. Internet users do not expect to be tracked across every single one of their internet-connected devices, including their web browser, apps, TVs, and more.

81. Indeed, the advent of privacy-preserving mechanisms like Apple's "Do Not Track" feature, which can prevent companies from collecting IDFA/ADID from individuals who opt-out, and similar features described above, has confirmed this expectation.

82. One study by Flurry Analytics (ironically) in 2021 shows that 88% of iOS users worldwide have availed themselves of this feature, indicating an intent to prevent apps from tracking them on their mobile devices.

83. Users do not know—and did not expect—that Yahoo would circumvent these protections by creating a new identifier that is even better than IDFA/ADID at tracking them across services.

84. Yahoo itself does not provide any information in its Privacy Policy for Plaintiff and Class Members to understand which websites or online services use ConnectID, such that they have no way of uncovering which services do or do not contain Yahoo's tracking technology.

85. Plaintiff and Class Members reasonably expected that their online activity would not be tracked by an unknown company, let alone that it would be used to target them across online services for profit.

86. Yahoo did not have consent to perform this type of omni-present cross-device tracking using Plaintiff's and Class Members' unique identifiers and private communications.

87. Its well-recognized that unique identifiers and other PII, like email addresses, have value. Even more valuable is the online activity data that companies like Yahoo obtain by tracking users through this information. This data is instrumental to updating and improving Yahoo's models and algorithms that identify and target unique users with advertisements.

YAHOO'S CONDUCT VIOLATES ESTABLISHED DATA PRIVACY REGIMES

88. The GDPR and CCPA both mirror Fair Information Practice Principles (FIPPs). Two of the core tenants of FIPPs are (1) clear user consent; and (2) data minimization.

89. Yahoo does neither of these things. Despite creating a cross-device persistent user

identifier, Yahoo makes zero effort to ensure Plaintiff and Class Members are even aware of where this technology is used. This is clear from its own Privacy Policy, which makes no attempt to identify the entities using its services or that Yahoo creates ConnectIDs based off their email addresses. This is directly at odds with Yahoo's representation that its ConnectID and advertising solutions are "[p]rivacy first" and respect "[c]onsumer choice."

90. Separately, the creation of an ever-present persistent identifier is inconsistent with the principle of data minimization, which requires that data should be stored and used only for the period of time in which that data is necessary. Indeed, the fact that device and user-specific identifiers are persistent (and not deleted) is exactly why even device identifiers like IDFA are being phased out by companies like Apple to preserve users' privacy. Yahoo's creation of ConnectID—a permanent and consistent identifier—is a regression from today's privacy norms.

TOLLING & CONCEALMENT

91. The earliest Plaintiff and Class Members could have discovered Yahoo's conduct was shortly before the filing of this Complaint. Plaintiff became aware of Yahoo's conduct through communications with counsel that are protected from disclosure.

92. Plaintiff and Class Members, despite their due diligence, could not have discovered Yahoo's conduct by virtue of how its technology works and its lack of disclosures.

93. Yahoo's interception of unique identifiers, including ConnectID, other personal data, and other identifiers, happens inconspicuously in the background. This process is undetectable to an ordinary person, highly technical, and prevented Plaintiff and any Class Member from uncovering it.

94. Yahoo had exclusive knowledge that ConnectID, its other identifiers, and its tracking technology were tracking Plaintiff and Class Members across the internet alongside their

private communications on third-party apps, websites, and other services. Similarly, Yahoo had exclusive knowledge that it was using this information to propagate one of the largest targeted advertising systems.

95. Yahoo's fraudulent conduct prevented Plaintiff and Class Members from discovering its conduct. Yahoo maintained a privacy policy that lacked adequate disclosures for Plaintiff and Class Members to uncover that Yahoo even intercepted, had, or used their data. Yahoo publicly held out its identifiers and technology as privacy-preserving mechanisms, even though they were not.

96. Yahoo was under a duty to disclose the nature and significance of its data interception and use practices—especially in light of its public statements—but did not do so. Yahoo is therefore, estopped from relying on any statute of limitations by virtue of the discovery rule and doctrine of fraudulent concealment.

CLASS ACTION ALLEGATIONS

97. Plaintiff brings this action under Fed. R. Civ. P. 23 individually and on behalf of the following Nationwide Classes:

> **Identifier Class:** All natural persons in the United States for whom Yahoo intercepted or assigned a ConnectID or other identifier.
>
> **Communications Class:** All natural persons in the United States who had their communications with third parties intercepted or used by Yahoo without their consent.

98. The Classes exclude: (1) any judge presiding over this action or their immediate families; (2) Yahoo, its subsidiaries, affiliates, parents, successors, predecessors, and any other entity in which Yahoo has a controlling interest; (3) Yahoo's current and former employees, officers, and directors; and (4) Plaintiff's and Yahoo's counsel.

99. ***Numerosity.*** While the precise size of the Classes is currently unknown to Plaintiff,

each of the Classes consists of well over a million individuals and members of each of the Classes can be identified through Yahoo's records.

100. ***Predominant Common Questions.*** The Classes' claims present several common questions of law and fact that predominant over questions (if any) that affect individual class members. This includes:

a. Whether Yahoo violated Plaintiff's and the Classes' privacy rights;

b. Whether Yahoo engaged in unfair and deceptive conduct;

c. Whether Yahoo's acts and practices violate the Pennsylvania Wiretapping and Electronic Surveillance Control Act;

d. Whether Plaintiff and Class Members are entitled to damages and/or equitable relief, including injunctive relief, restitution, and disgorgement; and

e. Whether Yahoo was unjustly enriched.

101. ***Typicality.*** Plaintiff's claims are typical of all Class Members because they arise from the same conduct and are based on the same legal theories.

102. ***Adequate Representation.*** Plaintiff will (and has) fairly and adequately represented the Classes and protected the interest of all Class Members. Plaintiff has retained competent counsel with significant experience in class action and data privacy litigation. Plaintiff and counsel have no interest that conflicts with the interests of the Classes and is not subject to any unique defenses. Plaintiff and his counsel will vigorously prosecute this action to advance the interest of the Classes and have the resources necessary to do so.

103. ***Substantial Benefits.*** A class action is superior to all other possible methods to fairly and efficiently adjudicate this case and controversy, and joinder of all Class Members is impracticable. Proceeding as a class case has significant advantages to individual litigation,

including: (1) comprehensive oversight by a single court, which avoids inconsistent outcomes; and (2) saving time and expense by litigating the same claims arising from the same conduct all in one action.

104. Plaintiff reserves all rights to revise or modify the class allegations based on facts and legal developments following additional investigation or discovery.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Violation of New York General Business Law § 349 ("GBL § 349")
On Behalf of the Plaintiff and Classes

105. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

106. Yahoo is considered a "business" under GBL § 349.

107. Yahoo' s business acts and practices are unfair and deceptive under GBL § 349. New York (as do other states through their respective unfair and deceptive trade practices statutes) has a strong public policy of protecting consumers' privacy interests, including protecting consumers' personal data. Yahoo violated GBL § 349 by, among other things, surreptitiously intercepting Plaintiff's and Class Members' email addresses through its tracking technology to create persistent identifiers (i.e., Yahoo ConnectIDs). Yahoo used the Yahoo ConnectIDs to track Plaintiff's and Class Members' activities and communications on all websites containing Yahoo's tracking technology and create user profiles for Plaintiff and Class Members for use in its advertising business.

108. Plaintiff and Class Members did not consent to Yahoo's conduct. At no time did Yahoo inform Plaintiff or Class Members that it was using their PII to track their activities and communications on other websites to create user profiles used for its advertising business.

109. Yahoo's business acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm of Yahoo's secret collection and use of their PII for advertising purposes is significant, and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiff and Class Members were completely unaware of Yahoo's conduct, they could not possibly have avoided the harm.

110. By collecting and using Plaintiff's and Class Members' PII, Yahoo has taken money or property from Plaintiff and Class Members and caused harm to Plaintiff's and Class Members' privacy interests. Plaintiff and Class Members seek all available damages under applicable state consumer protection laws, including statutory damages under GBL § 349.

SECOND CAUSE OF ACTION
Violation of Common Law Invasion of Privacy (Intrusion Upon Seclusion)
On Behalf of the Plaintiff and Classes

111. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

112. Intrusion upon seclusion requires pleading: (1) that the defendant intruded on a place, conversation, or matter in which plaintiff has a reasonable expectation of privacy; and (2) that the intrusion would be highly offensive to a reasonable person.

113. Yahoo's collection, interception, and use of Plaintiff's and Class Members' personally identifiable information constitutes an intentional intrusion. As does its use of this information to create "Identity Graphs," which are keyed off these identifiers to track and profile Plaintiff and Class Members based on their online activity.

114. Yahoo's interception and use of Plaintiff's and Class Members' private online communications, associated with their assigned ConnectID and other identifying information, is

likewise an intentional intrusion upon Plaintiff's and Class Members' solitude.

115. Plaintiff and Class Members reasonably expected their unique identifiers and other personal data, alongside their online activities, would not be intercepted or used by an unknown third party. The types of identifying information Yahoo stored in "Identity Graphs" are particularly private because they are often directly identifiable, permanent identifiers (e.g., IP address, phone number, email address). Plaintiff and Class Members reasonably expected this information would remain private and confidential and would not be intercepted or used by third parties without their consent.

116. This expectation is particularly heightened given that there were no disclosures of Yahoo's involvement in intercepting, processing, and using their unique identifiers and other personal data and online communications.

117. Plaintiff and Class Members did not consent to, authorize, or understand Yahoo's interception or use of their private data.

118. Yahoo's conduct is highly offensive because it violates established social norms. Consumers do not expect to be surveilled whenever they use the internet, especially in light of state laws requiring companies to make adequate disclosures regarding their collection and use of data.

119. Yahoo's conduct is particularly offensive in light of the secretive nature in which it takes place. Plaintiff and Class Members had no way of knowing Yahoo collected their unique identifiers and other personal data and other online communications, and Yahoo did so from thousands of websites, if not more.

120. Yahoo's conduct caused Plaintiff and Class Members harm and injury, including a violation of their privacy interests.

121. Plaintiff and Class Members seek damages to compensate the harm to their privacy interests, among other damages, as well as disgorgement of profits made by Yahoo as a result of its intrusion upon seclusion.

122. Since Defendant's conduct was willful, knowing, and carried out with a conscious disregard for Plaintiff's or Class Members' rights, Plaintiff and Class Members are entitled to punitive and exemplary damages.

123. Plaintiff and Class Members also seek any other relief the Court may deem just and proper.

THIRD CAUSE OF ACTION
Violation of Wiretapping and Electronic Surveillance Control Act (WESCA),
18 Pa. C.S. § 5701 *et seq*
On Behalf of Plaintiff and Class Members

124. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

125. The Pennsylvania legislature passed the Wiretapping and Electronic Surveillance Control Act ("WESCA") in order to prohibit any person from:

a. intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept any wire, electronic or oral communication;

b. intentionally disclosing or endeavoring to disclose to any other person the contents of any wire, electronic or oral communication, if that person knows or has reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or

c. intentionally using or endeavoring to use the contents of any wire, electronic or oral communication, if that person knows or has reason to know that the information was obtained through the interception of a wire, electronic or oral communication.

126. WESCA defines "electronic communication" as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system, except: (1) [d]eleted, (2) [a]ny wire or oral communication, (3) [a]ny communication made through a tone-only paging device, or (4) [a]ny communication from a tracking device (as defined in this section)." 18 Pa.C.S.A. § 5702. It further defines "intercept" as "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." *Id.*

127. Any person whose wire, electronic, or oral communication is intercepted, disclosed, or used in violation of WESCA "shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S. § 5725.

128. Yahoo qualifies as a person under the WESCA. *See* 18 Pa. C.S. §5702.

129. Yahoo's conduct, as described herein, violates WESCA.

130. Plaintiff and Class Members had a reasonable expectation of privacy in their private internet browsing data and were unaware that Yahoo was amassing their PII, using its ConnectID to track them across websites and apps, and further monetizing that data without their consent.

131. Yahoo intentionally inserted an electronic device into Plaintiff and Class Members devices without first obtaining their knowledge or consent.

132. Through the conduct described herein, Yahoo violated Plaintiff's and Class Members' statutorily protected privacy rights.

133. Under WESCA, Plaintiff and Class Members are entitled to recover:

a. actual damages but not less than liquidated damages computed at the rate of $100 per day for each violation or $1,000, whichever is higher;

b. punitive damages; and

c. a reasonable attorneys' fee and other litigation disbursements reasonably incurred.

FOURTH CAUSE OF ACTION
Unjust Enrichment
On Behalf of the Plaintiff and Classes

134. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

135. Yahoo receives benefits from Plaintiff and Class Members in the form of their unique identifiers and other personal data and private online communications. Yahoo acquired this information without Plaintiff's and Class Members' authorization and without providing corresponding compensation.

136. Yahoo acquired and used this private data for its own benefit, including tangible economic benefits from companies that used Yahoo for targeted advertising.

137. Had Plaintiff and Class Members known of Yahoo's misconduct, they would not have agreed Yahoo could acquire and use their private data.

138. Yahoo unjustly retained these benefits at the expense of Plaintiff and Class Members. Plaintiff and Class Members were harmed by this conduct and were not provided any commensurate compensation.

139. The benefits Yahoo received and derived from Plaintiff's and Class Members' private data rightly belong to Plaintiff and Class Members. It is inequitable under unjust enrichment principles for Yahoo to retain the profits and other intangible benefits they derived through its wrongful conduct.

140. Yahoo should be compelled to disgorge these profits and other inequitable proceeds

in a common fund for the benefit of Plaintiff and Class Members.

FIFTH CAUSE OF ACTION
Injunctive Relief
On Behalf of the Plaintiff and Classes

141. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

142. Yahoo's conduct has caused and continues to cause harm to Plaintiff's and Class Members' privacy and autonomy, as it continues to store unique persistent identifiers, as well as the private contents of their communications, on its own systems. Yahoo routinely uses this information for targeted advertising.

143. Accordingly, Plaintiff and Class Members seek injunctive relief, including an order permanently restraining Yahoo from continuing to use and store this information without consent and/or a court order, and requiring Yahoo to delete this information from its systems.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the putative Classes requests the Court enter an Order:

a. Certifying the Classes and appointing Plaintiff as Class Representative;

b. Finding Yahoo's conduct unlawful;

c. Awarding injunctive and other equitable relief as is just and proper;

d. Awarding Plaintiff and the Classes statutory, actual, compensatory, punitive, nominal, and other damages, as well as restitution and/or disgorgement of unjust and unlawful profits;

e. Awarding pre-judgment and post-judgment interest;

f. Awarding reasonable attorneys' fees, costs, and expenses; and

g. Granting any other relied as the Court sees just and proper.

Dated: April 9, 2025

/s/ Vicki J. Maniatis

Vicki J. Maniatis (NY Bar No. 2578896)
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
405 East 50th Street
New York, NY 10022
Tel.: (516) 491-4665
vmaniatis@milberg.com